FUN WITH APPLICATION SECURITY



Bruce Abernethy for BeerCityCode 2017





MY FIRST TIME CODING 1978





Programming on the P.E.T

FIRST SECURITY EXPERIENCE - 1988



.2E0			
DIM.	PASTAN	CARD DUDY (MUS	VERP (NKA
		VIERI	
MI 🚰			😎 e 🚺 🚺 I (10=
			bad a
	<u> </u>	Leten	
CON	Se	cond Edit	CONSSI! ENDIE
The	Art	of Bojontifie	Barmautino IIF (
		Dejentanje	Compacingen ins
NOX - NOVIN	ain ei i	Nitsia, XIIST, Bali	A Teokolaky
with	am T. V	eccerting ^{CON} Bris	n P. Flannery
	ERRMAX	BESSI H	ESSI*BESSIO(X)/BI
	ERRM	AX=MAX (ERBMAX, A)	BS (YEBR (J) /YSCAL (J
A (1+M00	CONTIN		SUBROUTINE PRE
2) MA (I)	ERRMAX	ERSMAX/EDS	PARAMETER (NPM
	IF (ERR	MAX.LT.ONE) THE	N DIMENSION DATA
FUTS	HDID		REGIN HDATA
		EQ.NUSE) THEN	CONTINUE
EG (NPM)	K) ES	SXT=H*SHRINK	DO 14 J=1,NFUT
	ELSE	IF(I.EQ.NUSE-1)) THEN DISCRP=0.
141	ELSE	CALER-GROW	DO 12 K-1 NB
		EXT- (H+NSEQ (NUS)	E-1)) SUM=SUM+D (
XTE=1		F ((N-INT (SQRT (FLOAT CONTINUE
XTP)		SS1 3=8,1,-1	DO 13 K=NPOLI
1910 1910	10042-12 2017-12	Past (J	CONTINUE
CON	LINUE		REG(1)=SUM
D.	SEAUL2	A P P P TAKE U ATT P TA A	The Extention Products





FREAK ATTACK



vptOr 2.0		
	Ooops, your files have been encrypted!	French
1	Qu'est-ce qui s'est passé avec mon ordinateur? Vorfalars importants cont duttris. Enauroug de von documers, photos, viden, barre de docusées et aut plus acteristicar de l'autoriste d'infinit Neur Arv que vous its e ocup moyors de récipient vou finiter, man perde par votre temps. Per récupiere vou fichairs namentes service de déregatage.	er fichiers ne m é à chercher un sonzie ne peut
t will be raised on 2017 205758 Time Left 13	Puis-je récupérer mes fichiers? 50. Nou vou generimme que vous prover récupérer tous vos fichi securit ét d'actionnes. Nais vous juit vous que avait de temp. Vous pouve décempter certain de vos fichiers grantement. Envoys cliquent me - d'enverpte. Nais it vous souhables décempter tous vos fichiers, vous deves payer. Vous it vous que à hors pour consumtre le paisment. Envirté, le prin a	ers en foute maistement en ers doublé
ies will be lost on 2017 20:57:50	En outre, il vour ne payes par dans 7 jours, vour ne poerter par trea pour toujours. Staus aurens des événements granuts pour les utilisateur 2 qui sont sig pouvaient par payer en 6 moit.	ofter son ficture sauvres qu'ils n
nmeten 13:57:50	Comment je paye? Le paiement en accepté uniquement dans Elicoin. Pour plus d'inform About biscoin: Ynullies viriller le richt acteut de Elicoin et acheter des bitcoins. Pour	ations, cliques : star
o Marra 2	Bitcoin KCCFTCD HISK 115p7UMMngejtpMvkpHijcRdfJNXj8LrL	s: n

Check Payment

Decrypt

Contact Us

Paym 5/1

02:

Your

About int

MAKE SOFTWARE DEVELOPMENT FUN AGAIN

CONTENT WARNING

WARNING: THE FOLLOWING CONTENT AND OPINIONS EXPRESSED ARE THOSE OF THE AUTHOR [BRUCE ABERNETHY] AND TO NOT REFLECT THOSE OF HIS EMPLOYER [MEIJER] OR [DISNEY/NICKJR]













WHAT MAKES IT "FUN"

- Automation
- "Al"
- Rules
- Tools



A Common Sense Approach to Web Usability FOREWORD BY ROGER BLACK







STRIDE AND DREAD

STRIDE

- Spoofing Identity,
- Tampering with Data,
- Repudiation,
- Information Disclosure,
- Denial of Service

DREAD

• Damage Potential,

(;) LOGIN

SON USER INFO

TICTACTOEGAME

- Reproducibility,
- Exploitability,
- Affected Users,
- Discoverability

THREAT MODEL

- Have a high-level design. Napkin to formal tool.
- Data is exposed in primarily three places
 - At rest wherever you store it
 - In memory when it is being used
 - In transit when it is moving
- Trust boundaries

WHAT'S NOT FUN

- Doing the diagram by hand (Visio, Paint, GIMP).
- Doing the analysis by hand.
- Easily missing something.
- Not having time.

THREAT MODELLING TOOL



0 0C2 Days TicheTes Threat Madeline Test 2016				
File Edit View Settings Diagram Reports Help	🗑 BC3 Dora	TicTacToe - Threat Modeling Tool 2016		×
	File Edit View Settings Diagram Reports Help			
	🗎 💾 🕛	$ \begin{array}{cccccccccccccccccccccccccccccccccccc$		
	Tic Tac Toe M	ain ×		•
	Threat List		1	Ψ×
	ID 🔹 C	ategory V Description	Priority	$\gamma \uparrow$
	41 S	poofing iOS App may be spoofed by an attacker and this may lead to unauthorized access to Web Service. Consider using a st.	High	
	42 Ta	ampering If iOS App is given access to memory, such as shared memory or pointers, or is given the ability to control what Web	High	
	43 Re	epudiation Web Service claims that it did not receive data from a source outside the trust boundary. Consider using logging or au	High	
User	44 D	enial Of Servi Web Service crashes, halts, stops or runs slowly; in all cases violating an availability metric.	High	
	45 D	enial Of Servi An external agent interrupts data flowing across a trust boundary in either direction.	High	
	16 FI	eviation Of Pr Web Service may be able to impersonate the context of iOS Ann. in order to gain additional privilege	High	, ×
		31 Threats Displayed, 31 Total		
	Threat Droport			
	mieat Propert			
	ID: 41 Di	agram: Tic Tac Toe Main Status: Not Started Y Last Modified	Genera	ated
	Title:	Spoofing the iOS App Process		
	Category:	Spoofing ~		
	Description:	iOS App may be spoofed by an attacker and this may lead to unauthorized access to Web Service. Consider using a standard authentica mechanism to identify the source process.	tion	
	Justification:			
Messages - No issues found Description	Interaction:	HTTPS		
	Priority:	High ~		
	Threat Proper	ties Notes - no entries		_
Marsager - No issues found Notes - no anti-				
messages no issues round mores no endres	-			_

OWASP THREAT DRAGON (BETA - X-PLAT)



SECURITY HAT ON

"Just because you are paranoid doesn't mean that they aren't watching you."





DESIGNING A SECURE APP

- Secure Coding "Level 0" is good coding.
- Much of malicious coding can appear at the outset like simply really bad coding practices
- Also User Interface
 - Well-meaning UI choices can be bad for security

INFORMATION DISCLOSURE

- Most is common sense
- Don't return error details
- Don't return info that could be used "for evil"

CREATE A NEW ACCOUNT	
spacemoses1337	
hunter Password is being used by /u/row	ealdo37189. Please choose another passwo
hunter	
email	

Password is being used by /u/rowealdo37189. Please choose another password.

I understand the risks of using someone else's password

OTHER GREAT (NOT) EXAMPLES

*	Secu	rity	Q	Jest	ioi

Please select your question... What is the Capitol of California? What is your favorite color? What is your favorite drink? What is your mother's maiden name? What was the make of your first car? What was your first pet's name? Who is your favorite superhero?

Security Question is required

To login simply type in your mobile number and password. The password is the last four digits of your mobile number.

*
*

login

By creating an account, you are agreeing to terms of use and privacy rights.

City of San Jose Parks, Recreation and Neighborhood Services Department: Terms of Use Your Privacy Rights

Active Network, LLC: Terms of Use Copyright Policy Your Privacy Rights

Create Account Create Account and Add Family Member

DESIGN GUIDANCE



OUDASP Open Web Application

Security Project

- OWASP Top 10
- SANS Top 25

WHAT'S NOT FUN

- Figuring this stuff out on your own
- It is wise to learn from your mistakes. It is wiser to learn from other people's mistakes

OWASP TOP 10

Open Web Application

Security Project

Injection

- Cross-Site Scripting (XSS):
- Vulnerability that is created from insecure coding techniques, resulting in improper input validation. Often used in conjunction with CSRF and/or SQL injection.

Insecure Direct Object References

 A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.





HELP WHILE CODING

- This is where the real fun happens
 - Adding features
 - Optimizing code

WHAT'S NOT FUN

- Reviewing 10,000 lines of code looking for patterns that might match common vulnerabilities (OWASP, SANS, etc.)
- Finding out after coding an entire feature that it has a fundamental security flaw and needs to be refactored or rewritten.
- Having the feature reach production and having to respond to a major incident.

TOOLS

- What tools should you have in your backpack, to help you along the way?
- "Anything that you might need, I've got inside for you."
- Binoculars, sticky tape
- Bag of Holding



STATIC ANALYSIS TOOLS

- Client-Side (Microsoft)
 - Roslyn,
 - Resharper,
 - DevSkim,
 - PumaScan
- Client-Side (VS Code, DevSkim)
 - Cross-platform



DEBUGGING WITH PROXIES

- We are going to cover our favorite proxies in just a few minutes when we are hacking our own code.
- Just remember that you can/could/should be using a proxy, where appropriate, even early while you are developing code ...



AUTOMATED TESTING - SECURITY TEST CASES

- Use Cases
- But also "Abuse Cases"
- Testing the happy path
- But also think about the unhappy path that "bad people" might take – more suggestions on how to do that coming soon too ...









NEVER CODE ALONE

0





CODING BUDDY

- Code & Coffee
- Personal Pull Requests





GITFLOW AND PULL REQUESTS ...





KNOW YOUR THREATS

- Script kiddies hobby opportunistic, not stealthy, known exploits
- Organized Crime hold hostage, profit possibly stealthy, often nontargeted / broad, zero-day – may target for corporate espionage
- Disorganized Crime petty theft, personal gain amateur, known
- Activist do damage, get press mixed, disgruntled
- Nation-state destabilize, do damage more skilled than you, targeted, precise, zero-day exploits

WHAT IS YOUR "GOLD"





MAN IN THE MIDDLE (MITM)

- CERT
- AES
- SSL/TLS Https everywhere (certificates in general)
- NIST
- YubiKey
- Oauth2 everywhere
- 2-factor multifactor
- nmap

TRAFFIC INSPECTION / INTERCEPTION

- Fiddler
- OWASP ZAP
- BURP Suite
- Swagger



BOTS

- Scanners
- Fuzzers
- Brute Force



	P	
	PIN	Freq
#1	1234	10.713%
#2	1111	6.016%
#3	0000	1.881%
#4	1212	1.197%
#5	7777	0.745%
#6	1004	0.616%
#7	2000	0.613%
#8	4444	0.526%
#9	2222	0.516%
#10	6969	0.512%
#11	9999	0.451%
#12	3333	0.419%
#13	5555	0.395%
#14	6666	0.391%
#15	1122	0.366%
#16	1313	0.304%
#17	8888	0.303%
#18	4321	0.293%
#19	2001	0.290%
#20	1010	0.285%



RED TEAM / BLUE TEAM



Hack yourself and/or your coding buddy.



BLUE TEAM

- Lesser known, but also cool.
- Ideas like Honeypots



BLUE TEAM FIELD MANUA



Blue Team Handbook: Incident Response Edition

A condensed field guide for the Cyber Security Incident Responder



Don Murdoch, GSE, MBA, CISSP + 15





bruce.abernethy@protonmail.com



-----BEGIN PGP PUBLIC KEY BLOCK-----Version: OpenPGP.js v2.3.8 Comment: http://openpgpjs.org

xsBNBFkQ9dcBCADM9qNu8YgSZhvaw7q/h6L61DXS71+rsFEazEMtD5P/NTVV B/VKfnO3sXGhNs1hsGkpHtdTgfwhVkh9og5oDIS1RupnH262r1P/3fqwQ9Zx fDalY41IxBk2UgiL8+oDqY85YeJyGuCmLC+S/p/fBBKQn2qO1IL+NDg/C6kM HrfZebIEwEy9NxCInfU5xshIftwnOzniyzYa1XMcri1A++LQm6pY9pq433fb gvEtvcLNAAQyusutXFHNECwVn++jcntrY/G8/30krcDPwMumxCZRUwfXGrNm anxF+VTGvCPpuHMoqgZMtJ+BSSEPCTY2wcemF5gYTUcDL4DfvenKn5Q5ABEB AAHNP2JydWN1LmFiZXJuZXRoeUBwcm90b25tYW1sLmNvbSA8YnJ1Y2UuYWJ1 cm5ldGh5QHByb3Rvbm1haWwuY29tPsLAdQQQAQgAKQUCWRD12AYLCQcIAwIJ EH4Y4k7JFhhhBBUICgIDFgIBAhkBAhsDAh4BAABb6wf/Y6APqS1GPBHGvV6X PPpyZLVOgVa6gQexLz/5pcRlaWHA4tb/bIzyWSh27Xq6KQkKEAi99uXEoDiw fQbF2+gw0LDhUoOXV1Qh5ZVmuKrQt2G8gP1qqTk2M0NRjFemGtQt+/Gr5yCa Tay/94jhyHaciCcJs4HHLT4yK90/xJZBfnUIkFxNegRGA0ZCe+gg7zQRXDcA kBaKtUwk7aBiN4AHd2NlGt86k/HG/Aug98IZaA6ISm/SfiSEaJLp2jOb+FHs z8PxjvzfveSZKKROamRxm9Vpspv66xkCdZKhrhG/P8cBsWL9S5tSddcZwh4V lKzSvQ5cgbwj40EpuG3aM1siI87ATQRZEPXXAQgA0SKe1zscea92E3Bzfpmo omcgDCsySpxdIwYHszXbi/0P76/fWxg40VVq4vhBthfeUJjUQzcq/dUba6bc oOiYPAJMttQlAbS3nPWJc43KFtuIlQPkk5z6BgMu3kSRXSAK1qJFimvro1ns 1/dZeng1nofmLsCLDPm6Y3VepZks6oTsbdgXbAoBo3D2v7Je76u+x1Uc2ax0 g2VQo8oHXYvcw7e3BysrkyD4RkTYBw4m0YvqBSMSb1RrXxnuTxyH0rQGPvSQ 1CfaRI4NuMd0AtKvJ9hIhNn+DxcswWkk/T+1yB3C+/ZEsHhVgGWTJ0XnCfM8 R000EbVJr3LmfI6g4MRHRwARAQABwsBfBBgBCAATBQJZEPXYCRB+G0J0yRYY YQIbDAAAHs0H/1m3zx8W9KvXXz0Ue6Nbo59CP922EqEHhB7tIgikjQS3khko OQcgtNnhXr2LhZvKVxJC202sLB268znWqgXLinzPUq7euqA2PiG9K9/e38Fv euxcGoDPb7do0CQF0IbowMF7yBho2BYYHtA9pgi9bPjII1zs6XARIVRhIWRs c3BsXFYfpk8yvo2ulX18iP5Yh1NV+p8quuZhrt60Co10fpcam5kq4i0AiyBu LALkalbBho6Ruk82SSXQ01Ks6zU95ZsAZT0xcUhKsCxMKIpx4fkblrH+149c x04fomhZg3vqiUVhxVDQGN9oJzUtOtmPtjLZ9jFAiyErBt8jvbfEsrg=

=9XpN

----END PGP PUBLIC KEY BLOCK-----

"FREE" SERVICES

- There is no such thing as a free lunch.
- You are "paying" with your privacy, and security.



FACEBOOK & YOU

If you're not paying for it, you're not the customer. You're the product being sold

OTHER FUN THINGS ... IF I TALK TOO FAST

- YubiKey
- BashBunny